Attorney Docket # 2132-56PCON

Patent

#10

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of
Jarmo MIETTINEN et al.
Serial No.: 09/977,669
Filed: October 15, 2001
For: Management of an Identity Module

LETTER TRANSMITTING PRIORITY DOCUMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

SIR:

In order to complete the claim to priority in the above-identified application under 35 U.S.C. §119, enclosed herewith is a certified copy of each foreign application on which the claim of priority is based: Application No. **990846,** filed on April 15, 1999, in Finland; International Application No. **PCT/FI00/00328,** filed on April 17, 2000.

Respectfully submitted,

COHEN, PONTANI, LIEBERMAN & PAVANE

By _____

Lance J. Lieberman
Reg. No. 28,437
551 Fifth Avenue, Suite 1210
New York, New York 10176
(212) 687-2770

Dated: May 29, 2002

PATENTTI- JA REKISTERIHALLITUS
NATIONAL BOARD OF PATENTS AND REGISTRATION

Helsinki 07.03.2002

E T U O I K E U S T O D I S T U S
P R I O R I T Y D O C U M E N T

Hakija
Applicant

1. **Sonera Smarttrust Oy, Helsinki, FI**
2. **Miettinen, Jarmo, Espoo, FI**
3. **Liukkonen, Jukka, Helsinki, FI**
4. **Nordberg, Marko, Helsinki, FI**

Kansainvälinen patenttihakemus nro
International patent application no **PCT/FI00/00328**

Kansainvälinen tekemispäivä
International filing date **17.04.2000**

Etuoikeushak. nro
Priority from appl. **FI 990846**

Tekemispäivä
Filing date **15.04.1999**

Keksinnön nimitys
Title of invention

"Management of an identity module"

Täten todistetaan, että oheiset asiakirjat ovat tarkkoja jäljennöksiä kansainvälisiä patenttihakemuksia vastaanottavana viranomaisena toimivalle Patentti- ja rekisterihallitukselle alkuaan annetuista selityksestä, patenttivaatimuksista, tiivistelmästä ja piirustuksista sekä niihin tehdyistä korjauksista.

This is to certify that the annexed documents are true copies of the description, claims, abstract and drawing, originally filed with the Finnish Patent Office acting as receiving Office for the international patent applications, and of any corrections thereto.

Pirjo Kaila
Tutkimussihteeri

Maksu 50 €
Fee 50 EUR

Osoite: Arkadiankatu 6 A
Address: P.O.Box 1160
FIN-00101 Helsinki, FINLAND

Puhelin: 09 6939 500
Telephone: + 358 9 6939 500

Telefax: 09 6939 5204
Telefax: + 358 9 6939 5204

HOME COPY

PCT REQUEST

13214S

Original (for **SUBMISSION**) - printed on 17.04.2000 02:49:01 PM

0 0-1	**For receiving Office use only** International Application No.	PCT/FI 0 0 / 0 0 3 2 8
0-2	International Filing Date	17 APR 2000 (17-04-2000)
0-3	Name of receiving Office and "PCT International Application"	The Finnish Patent Office PCT International Application
0-4 0-4-1	**Form - PCT/RO/101 PCT Request** Prepared using	PCT-EASY Version 2.90 (updated 08.03.2000)
0-5	**Petition** The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty	
0-6	**Receiving Office (specified by the applicant)**	National Board of Patents and Registration (Finland) (RO/FI)
0-7	**Applicant's or agent's file reference**	13214S
I	**Title of invention**	MANAGEMENT OF AN IDENTITY MODULE
II II-1 II-2 II-4 II-5 II-6 II-7	**Applicant** This person is: Applicant for Name Address: State of nationality State of residence	 applicant only all designated States except US SONERA SMARTTRUST OY c/o Sonera Oyj P.O.Box 106 FIN-00051 Sonera Finland FI FI
III-1 III-1-1 III-1-2 III-1-4 III-1-5 III-1-6 III-1-7	**Applicant and/or inventor** This person is: Applicant for Name (LAST, First) Address: State of nationality State of residence	 applicant and inventor US only MIETTINEN, Jarmo Everstinkatu 1 C 72 FIN-02600 Espoo Finland FI FI

PCT REQUEST

13214S

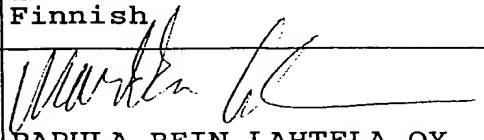
Original (for **SUBMISSION**) - printed on 17.04.2000 02:49:01 PM

III-2	**Applicant and/or inventor**	
III-2-1	This person is:	applicant and inventor
III-2-2	Applicant for	US only
III-2-4	Name (LAST, First)	LIUKKONEN, Jukka
III-2-5	Address:	Männikkötie 9 G 53 FIN-00630 Helsinki Finland
III-2-6	State of nationality	FI
III-2-7	State of residence	FI
III-3	**Applicant and/or inventor**	
III-3-1	This person is:	applicant and inventor
III-3-2	Applicant for	US only
III-3-4	Name (LAST, First)	NORDBERG, Marko
III-3-5	Address:	Itämerenkatu 12 D 74 FIN-00180 Helsinki Finland
III-3-6	State of nationality	FI
III-3-7	State of residence	FI
IV-1	**Agent or common representative; or address for correspondence** The person identified below is hereby/has been appointed to act on behalf of the applicant(s) before the competent International Authorities as:	agent
IV-1-1	Name	PAPULA REIN LAHTELA OY
IV-1-2	Address:	P.O. Box 981 (Fredrikinkatu 61 A) FIN-00101 Helsinki Finland
IV-1-3	Telephone No.	+358 9 3480 060
IV-1-4	Facsimile No.	+358 9 3480 0630
IV-1-5	e-mail	papula@papula.fi
V	**Designation of States**	
V-1	Regional Patent (other kinds of protection or treatment, if any, are specified between parentheses after the designation(s) concerned)	AP: GH GM KE LS MW SD SL SZ TZ UG ZW and any other State which is a Contracting State of the Harare Protocol and of the PCT EA: AM AZ BY KG KZ MD RU TJ TM and any other State which is a Contracting State of the Eurasian Patent Convention and of the PCT EP: AT BE CH&LI CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE and any other State which is a Contracting State of the European Patent Convention and of the PCT OA: BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG and any other State which is a member State of OAPI and a Contracting State of the PCT

PCT REQUEST

13214S

Original (for **SUBMISSION**) - printed on 17.04.2000 02:49:01 PM

V-2	National Patent (other kinds of protection or treatment, if any, are specified between parentheses after the designation(s) concerned)	AE AG AL AM AT AU AZ BA BB BG BR BY CA CH&LI CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW	
V-5	**Precautionary Designation Statement** In addition to the designations made under items V-1, V-2 and V-3, the applicant also makes under Rule 4.9(b) all designations which would be permitted under the PCT except any designation(s) of the State(s) indicated under item V-6 below. The applicant declares that those additional designations are subject to confirmation and that any designation which is not confirmed before the expiration of 15 months from the priority date is to be regarded as withdrawn by the applicant at the expiration of that time limit.		
V-6	**Exclusion(s) from precautionary designations**	NONE	
VI-1	**Priority claim of earlier national application**		
VI-1-1	Filing date	15 April 1999 (15.04.1999)	
VI-1-2	Number	990846	
VI-1-3	Country	FI	
VII-1	**International Searching Authority Chosen**	Swedish Patent Office (ISA/SE)	
VIII	**Check list**	number of sheets	electronic file(s) attached
VIII-1	Request	4	-
VIII-2	Description	14	-
VIII-3	Claims	3	-
VIII-4	Abstract	1	13214s.txt
VIII-5	Drawings	2	-
VIII-7	TOTAL	24	
	Accompanying items	paper document(s) attached	electronic file(s) attached
VIII-8	Fee calculation sheet	✓	-
VIII-10	Copy of general power of attorney	✓	-
VIII-16	PCT-EASY diskette	-	diskette
VIII-18	**Figure of the drawings which should accompany the abstract**	1	
VIII-19	**Language of filing of the international application**	Finnish	
IX-1	**Signature of applicant or agent**		
IX-1-1	Name	PAPULA REIN LAHTELA OY	
IX-1-2	Name of signatory	Markku Simmelvuo	

PCT REQUEST

13214S

Original (for **SUBMISSION**) - printed on 17.04.2000 02:49:01 PM

FOR RECEIVING OFFICE USE ONLY

10-1	**Date of actual receipt of the purported international application**	17 APR 2000 (17 -04- 2000)
10-2	**Drawings:**	
10-2-1	Received	
10-2-2	Not received	
10-3	**Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application**	
10-4	**Date of timely receipt of the required corrections under PCT Article 11(2)**	
10-5	**International Searching Authority**	ISA/SE
10-6	**Transmittal of search copy delayed until search fee is paid**	

FOR INTERNATIONAL BUREAU USE ONLY

11-1	**Date of receipt of the record copy by the International Bureau**	

TILAAJAIDENTITEETTIMODUULIN HALLINTA

TEKNIIKAN ALA

Keksintö kohdistuu tietoliikennejärjestelmiin ja -laitteisiin. Erityisesti keksinnön kohteena on menetelmä identiteettimoduulin hallitsemiseksi ja identiteettimoduuli, joka käsittää välineet sen muistialueiden hallitsemiseksi.

Keksinnön kohteena on menetelmä identiteettimoduulille tallennettujen varmenteiden hallitsemiseksi. Menetelmässä vastaanotetaan identiteettimoduulille varmenne, ja tallennetaan mainitusta varmenteesta tietoa identiteettimoduulille.

KEKSINNÖN TAUSTAA

Matkaviestinverkot, esimerkiksi GSM-verkot (GSM, Global System for Mobile communications) ovat viime aikoina saavuttaneet suuren suosion. Matkaviestinverkkoihin liittyvät lisäpalvelut ovat lisääntyneet vastaavasti yhä kiihtyvällä vauhdilla. Sovellusalueet voivat olla mitä erilaisempia. Matkapuhelinta voidaan käyttää muun muassa pienten ostosten, esimerkiksi virvoitusjuoma- ja autopesuautomaattien maksuvälineenä. Arkipäiväisiä toimintoja, kuten maksutoiminteita, pankkipalveluita ja niin edelleen, on lisätty ja tullaan vastaisuudessakin lisäämään nykyisten matkaviestimien palveluvalmiuteen. Seuraavan sukupolven matkaviestimet tulevat olemaan edellisiään huomattavasti palvelutasoltaan ja tiedonsiirtokapasiteetiltaan kehittyneempiä.

Nykyisin on tunnettua käyttää digitaalista GSM-matkaviestintä tai muuta sähköistä ja langatonta päätelaitetta, jolla on ainutkertainen identiteetti, kaupallisiin transaktioihin, kuten laskun tai maksun maksamiseen sähköisesti. Patenttijulkaisusta US 5,221,838 tunnetaan laite, jota voidaan käyttää maksa-

miseen. Julkaisussa on kuvattu sähköinen maksujärjestelmä, jossa maksupäätteenä käytetään langattomaan ja/tai langalliseen tiedonsiirtoon kykenevää päätelaitetta. Julkaisun mukaiseen päätelaitteeseen kuuluu kortinlukija, näppäimistö, ja viivakoodin lukija tietojen syöttämiseksi ja näyttö maksuinformaation esittämiseksi.

Patenttijulkaisusta WO 94/11849 tunnetaan menetelmä tietoliikennepalveluiden käyttämiseksi ja maksuliikenteen suorittamiseksi matkapuhelinjärjestelmällä. Julkaisussa kuvataan järjestelmä, johon kuuluu päätelaite, joka on yhteydessä televerkon kautta palveluntarjoajan keskustietokoneeseen, joka sisältää palveluntarjoajan maksujärjestelmän. Matkapuhelinverkon päätelaitteeseen eli matkaviestimeen voidaan lisätä tilaajan tunnistusyksikkö, joka käsittää tilaajatiedot tilaajan tunnistamiseksi ja teleliikenteen salaamiseksi. Tiedot voidaan lukea päätelaitteeseen käytettäväksi matkaviestimissä. Esimerkkinä julkaisussa mainitaan GSM-järjestelmä, jossa käytetään tilaajaidentiteettimoduulia tai SIM-korttia (Subscriber Identity Module, SIM) tilaajan tunnistusyksikkönä.

Julkaisun WO 94/11849 mukaisessa järjestelmässä matkaviestin on yhteydessä matkapuhelinverkon tukiasemaan. Julkaisun mukaan yhteys muodostetaan tukiasemasta edelleen maksujärjestelmään ja maksettava määrä samaten kuin tilaajan tunnistamiseen tarvittava data välitetään maksujärjestelmään. Julkaisussa kuvatussa pankkipalvelussa asiakas asettaa pankin palvelukortin, joka sisältää SIM-yksikön, GSM-verkon päätelaitteeseen. Puhelinperustaisessa pankkipalvelussa päätelaite voi olla standardin mukainen GSM-matkaviestin. Julkaisussa kuvatulla menetelmällä voidaan käyttää langatonta tietoliikenneyhteyttä maksujen ja/tai laskujen tai muiden vastaavien pankkipalvelujen tai kassapalvelujen toteuttamiseen. Maksupäätteenä voitaisiin käyttää myös jotain muuta päätelaitetta.

Tärkeää on, että päätelaite sisältää tai siihen voidaan liittää jokin identiteettimoduuli, jolla on oma uniikki identiteettinsä. Se voi olla myös erillinen turvallinen piiri tai vastaava.

Digitaalisella allekirjoituksella, jota pidetään yleisenä vaatimustasona sähköisessä maksamisessa, varmistetaan välitettävän aineiston eheys ja lähettäjän alkuperä. Digitaalinen allekirjoitus muodostetaan salaamalla välitettävästä aineistosta laskettu tiiviste lähettäjän salaisella avaimella. Koska kukaan muu ei tunne lähettäjän salaista avainta, voi vastaanottaja purkaessaan salauksen lähettäjän julkista avainta käyttäen varmistua siitä, että aineisto on muuttumaton ja lähettäjän tuntemallaan salaisella avaimellaan muodostama. Eräs esimerkki digitaalisessa allekirjoituksessa käytettävästä algoritmista on RSA-salausalgoritmi, joka on julkisen ja salaisen avaimen salausjärjestelmä ja jota käytetään myös viestien salaamiseen.

Jotta voidaan käyttää yhtenäisiä menettelyjä kaupan tai muun sopimuksen osapuolten luotettavaan tunnistamiseen tietoliikenneverkolla, tarvitaan sähköinen identiteetti ja keinot identiteetin todistamiseen ja toteamiseen. Tällainen sähköinen identiteetti voi olla myös ns. verkkoidentiteetti (Net-ID, Network Identity). Sähköinen identiteetti perustuu älykortilla, tilaajaidentiteettimoduulilla, sähköisellä turvallisella piirillä tai vastaavalla oleviin henkilötietoihin ja avainpariin, salaiseen avaimeen ja julkiseen avaimeen, joka on tallennettu varmennehakemistoon luotetulle kolmannelle osapuolelle. Tällaisella tekniikalla voidaan toteuttaa viranomaisille ja muille palveluntarjoajille riittävän turvallisesti mm. osapuolten tunnistus, sähköinen allekirjoitus, salakirjoittaminen ja asioinnin kiistämättömyys.

Tässä hakemuksessa identiteetillä tarkoitetaan henkilöön tai identiteetin haltijana olevaan oi-

keushenkilöön liitettävää yksilöivää tietoa, jonka avulla henkilö tai haltija voidaan tunnistaa. Samaten identiteetillä voidaan tarkoittaa sovellusta tai palvelua tarkoittavaa yksilöivää tietoa, jonka avulla sovellus tai palvelu voidaan tunnistaa.

Julkisen avaimen menetelmässä käyttäjä säilyttää salaisen avaimen ainoastaan omassa hallussaan ja julkinen avain on yleisesti saatavilla. Ei riitä, että julkinen avain talletetaan sellaisenaan julkiseen hakemistoon, esimerkiksi x.500- tai LDAP-hakemistoon, koska joku saattaisi väärentää sen ja esiintyä sen jälkeen avaimen oikean haltijan nimissä. Sen sijaan tarvitaan varmennuspalvelua ja varmennetta, joka on luotetun tahon (varmentaja) todistus siitä, että nimi, henkilön tunnus ja julkinen avain kuuluvat samalle henkilölle. Varmenne on yleensä henkilön julkisesta avaimesta, nimestä, henkilötunnuksesta ym. tiedoista muodostuva kokonaisuus, jonka varmentaja allekirjoittaa omalla salaisella avaimellaan.

Kun sähköisesti allekirjoitetun sanoman vastaanottaja haluaa varmistua sanoman aitoudesta, hänen on ensin hankittava käyttöönsä lähettäjän varmenne, josta hän saa tämän julkisen avaimen ja nimen. Sen jälkeen hänen on todennettava varmenteen oikeellisuus. Tätä varten hänen on mahdollisesti hankittava käyttöönsä vielä muita varmenteita (varmenneketju), joita on käytetty kyseisen varmenteen varmentamiseen.

Jos varmenne on aito, vastaanottaja todentaa sanoman allekirjoituksen lähettäjän varmenteessa saamallaan julkisella avaimella. Jos allekirjoitus läpäisee testin, lähettäjä on varmenteen osoittama henkilö. Varmenteiden käyttöön liittyy myös sulkulista, jolle merkitään käytöstä poistetut varmenteet. Varmenteita ja sulkulistaa varten tarvitaan hakemistopalvelut.

Kun identiteettimoduulille tallennetaan erilaisia sovelluksia, joita käytetään sähköiseen maksamiseen, kaupankäyntiin, pankkiasioiden hoitamiseen

yms., tallennetaan samalla näiden sovellusten käyttämien palveluntarjoajien, kuten kaupan, pankin ja muiden sähköisiä palveluita tarjoavien organisaatioiden palvelussa käyttämät julkiset avaimet. Julkisia avaimia voidaan myös tallentaa myöhemmin riippuen tilaajaidentiteettimoduulin käyttäjän käyttämistä palveluista. Tällöin identiteettimoduulin käyttäjän ei erikseen tarvitse hakea varmennetta jokaista transaktiota varten, vaan varmenne on valmiina identiteettimoduulilla.

Mitä pidempi varmennusketju varmenteen muodostamiseen on syntynyt, sitä enemmän tietoa tarvitaan varmenteen tarkistamiseksi. Paljon muistia kuluttavat varmenteet ovat ongelmallisia nykyisille identiteettimoduuleille, koska identiteettimoduulin muistialue on usein rajattu. Tämä rajoittaa merkittävästi identiteettimoduulin käyttämistä erilaisiin palveluihin, joilla on eri varmenne. Näin ollen olisikin tärkeää, että varmenteen kokoa voitaisiin rajoittaa ja siten saada useampia varmenteita mahtumaan yhdelle identiteettimoduulille. Yksi palvelusovellus identiteettimoduulilla voi käyttää useita eri varmenteita asioidessaan käyttäjän puolesta eri palveluntarjoajien palveluissa. Näin ollen identiteettimoduulilla käytettävien eri palveluiden määrää rajoittaa miltei yksinomaan varmenteiden koko.

KEKSINNÖN TARKOITUS

Esillä olevan keksinnön tarkoituksena on poistaa tai ainakin merkittävästi lieventää edellä esitettyjä ongelmia. Erityisesti esillä olevan keksinnön tarkoituksena on tuoda esiin menetelmä ja identiteettimoduuli, joilla varmenteen koko pystytään määräämään tai ainakin kokoa voidaan supistaa, jolloin matkaviestinympäristössä käytettävien varmenteiden lukumäärää yhdellä identiteettimoduulilla voidaan kasvattaa.

Lisäksi keksinnön tarkoituksena on tuoda esiin menetelmä, jota käyttäen identiteettimoduulille voidaan tallentaa aikaisempaa useampia varmenteita katkaisematta luottamusketjua varmenneketjussa.

Esillä olevan keksinnön tunnusomaisten piirteiden osalta viitataan oheisiin patenttivaatimuksiin.

KEKSINNÖN YHTEENVETO

Keksinnön mukaisen ratkaisun toiminnan pääperiaatteena on tallentaa identiteettimoduulille. tallennettavat varmenteet siten, että niistä poistetaan varmenneketjun sisältämät varmenteet. Identiteettimoduuli voi olla SIM (Subscriber Identity Module, SIM), WIM (Wireless Identity Module, WIM), turvamoduuli tai muu vastaava erillinen turvallinen piiri tai sen tapainen identiteetin ilmaiseva laite tai komponentti. Identiteettimoduuli voi olla kiinteä tai irrotettava ja sen on oltava identiteetin omistajan hallittavissa Tallennus voidaan tehdä, jos identiteettimoduulille tallennetulla korttivarmenteella pystytään todentamaan oikeaksi identiteettimoduulille vastaanotettu varmenne. Kun varmenneketju on poistettu, jäljelle jäävä julkinen avain ja siihen liittyvä identiteetti tallennetaan suojatulle muistialueelle, jonne ei muilla sovelluksilla kuin korttivarmenteen käyttämällä sovelluksella ole pääsyä. Aina kun identiteettimoduulilla oleva palvelusovellus haluaa käyttää kortille tallennettua varmennetta, se pyytää sitä suojatulta muistialueelta korttivarmenteen käyttämältä sovellukselta. Korttivarmenteen käyttämä sovellus varmentaa suojatulta muistialueelta luetun varmenteen ja kun käyttäjä luottaa korttivarmenteen antajaan, voi käyttäjä luottaa myös kortilta luettuun varmenteeseen.

Keksinnön perusajatus voidaan kiteyttää vielä seuraavasti. Jokin toiminnallinen yksikkö on jaettu kahteen osaan A ja B sekä ehtoon C. Toiminnallinen yksikkö voi olla identiteettimoduulin muistilaite tai

muisti ja ehto C voi olla suodatin tai algoritmi, joka hallitsee muistialuetta. Osan A toiminta on tunnettu, avoin muistialue, ja sen toiminnallisuuksiin voidaan vaikuttaa tunnetuilla ohjeilla, identiteettimoduulin käyttöjärjestelmällä. Osa B voi toimia samalla tavalla kuin osa A, mutta B:n toiminnallisuuksia voi käyttää vain ehdot C tunteva. Tässä tapauksessa ehdon C tuntee vain korttivarmenteen antava varmenneviranomainen D ja kortilla oleva suodatin tai algoritmi, joka hallitsee suojattua muistialuetta.

Kun identiteettimoduulille tallennetaan uusi varmenne, pyytää uuden varmenteen luovuttaja varmenneviranomaiselta D varmenteensa tallennusta identiteettimoduulille. Varmenneviranomainen D autentikoi toiselta varmenneviranomaiselta E saadun uuden varmenteen ja poimii varmenteesta vain ne komponentit F, jotka välttämättä tarvitaan identiteettimoduulille tallennettavaksi.

Varmenneviranomainen D muodostaa E:n antamasta uudesta varmenteesta ja poimimistaan komponenteista F oman varmenteensa G. Varmenteesta G arkistoidaan hakemistoon tarvittavat tiedot, jotta voidaan lukea, mistä varmenteesta aineisto F on luotu ja todeta, että aineisto on varmenneviranomaisen D varmentama.

Koska vain varmenneviranomainen D tuntee ehdot, miten F sijoitetaan suojatulle alueelle B, voidaan F tulkita varmenteeksi, joka ei ole julkinen ja johon voidaan luottaa.

Keksinnön mukaisessa menetelmässä identiteettimoduulille tallennettujen varmenteiden hallitsemiseksi vastaanotetaan identiteettimoduulille varmenne ja tallennetaan mainitusta varmenteesta tietoa mainitulle identiteettimoduulille. Identiteettimoduuli käsittää tietojenkäsittelylaitteen muistilaitteen, joka on yhdistetty mainittuun tietojenkäsittelylaitteeseen, muistilaitteelle tallennetun korttivarmenteen, sovelluksen, joka käyttää identiteettimoduulille tallennet-

tuja varmenteita ja tiedonsiirtolaitteen, joka on yhdistetty mainittuun tietojenkäsittelylaitteeseen ja johon on järjestetty liityntärajapinta tiedon siirtämiseksi ulkoisen laitteen, kuten matkaviestimen, ja identiteettimoduulin välillä.

Keksinnön mukaisesti todennetaan mainittu varmenne oikeaksi mainitulla korttivarmenteella ennen varmenteen tallentamista ja suodatetaan mainitusta oikeaksi todennetusta varmenteesta sen sisältämä varmenneketju. Ennen suodatusta voidaan vielä erikseen tarvittaessa varmentaa jokainen varmenneketjun allekirjoitus ja varmenne. Suodatuksen jälkeen varmenteesta jää tallennettavaksi sen sisältämä julkinen avain ja siihen liittyvä identiteetti, mutta myös muita tietoja voidaan tallentaa. Tällä tavalla voidaan merkittävästi pienentää varmenteen käyttämän muistin määrää. Kun varmennetta halutaan käyttää, on se ensin varmennettava korttivarmenteella.

Keksinnön eräässä sovelluksessa hylätään mainittu varmenne, jos se todennetaan epäluotettavaksi ennen sen tallentamista tai ennen sen käyttöä. Kun vielä käytetään luotettavia välineitä ja ohjelmistoja, voidaan täten varmenteisiin ja niillä tehtyihin transaktioihin luottaa. Kuitenkin tässä huomautamme, että jos korttivarmenne hylätään, se ei välttämättä tarkoita sitä, että varmennetta ei voisi käyttää jokin kortilla oleva sovellus. Tällöin, jos jokin sovellus varmenteen tunnistaa, se voidaan tallentaa identiteettimoduulille. Ainoa ero suodatettuun varmenteeseen on, että varmenne tallennetaan kokonaisena suodattamatta siitä mitään pois.

Keksinnön mukainen identiteettimoduuli varmenteiden hallitsemiseksi käsittää edellä mainitut komponentit. Lisäksi identiteettimoduuli käsittää välineet varmenteen vastaanottamiseksi identiteettimoduulille ja välineet mainitun varmenteen sisältämän tiedon tallentamiseksi muistilaitteelle.

Keksinnön mukaisesti identiteettimoduuli käsittää välineet varmenteen todentamiseksi oikeaksi mainitulla korttivarmenteella ennen varmenteen tallentamista ja välineet oikeaksi todennetun varmenteen sisältämän varmennusketjun suodattamiseksi varmenteesta. Edelleen identiteettimoduuli käsittää välineet varmenteen varmentamiseksi korttivarmenteella ennen sen käyttämistä.

Keksinnön eräässä sovelluksessa identiteettimoduuli edelleen käsittää välineet varmenteen hylkäämiseksi, jos se todennetaan epäluotettavaksi ennen sen tallentamista, ja välineet varmenteen hylkäämiseksi, jos se todennetaan epäluotettavaksi ennen sen käyttämistä. Edelleen identiteettimoduuli voi käsittää välineet jokaisen mainittuun varmenteeseen sisältyvän allekirjoituksen todentamiseksi ennen suodatusta.

Esillä olevan keksinnön etuna tunnettuun tekniikkaan verrattuna on, että varmenteita voidaan sijoittaa rajoitetulle muistille entistä enemmän. Erityisesti keksinnön ansiosta identiteettimoduulille tai älykortille voidaan tallentaa useampi varmenne.

Edelleen keksinnön etuna tunnettuun tekniikkaan verrattuna on, että identiteettimoduulin päivitys uusilla varmenteilla ja sovelluksilla voidaan varmentaa keksinnön mukaisella varmistusmenetelmällä korttivarmennetta käyttäen.

KUVALUETTELO

Seuraavaksi keksintöä selostetaan suoritusesimerkkien avulla viittaamalla oheiseen piirustukseen, jossa

kuvio 1 esittää kaaviomaisesti erästä esillä olevan keksinnön mukaista identiteettimoduulia,

kuvio 2 esittää kaaviomaisesti erästä keksinnön mukaista menetelmää varmenteen tallentamiseksi identiteettimoduulille, ja

kuvio 3 esittää kaaviomaisesti sanomarakennetta, jota voidaan käyttää esillä olevan keksinnön mukaisessa menetelmässä.

Vaikka seuraavissa esimerkeissä keksintöä selostetaan viitaten tilaajaidentiteettimoduuliin, niin keksintöä voidaan käyttää minkä tahansa päätelaitteen, joka käyttää edellä mainittuja identiteettimoduuleita, yhteydessä. Keksintö ei rajoitu pelkästään GSM-verkon tilaajaidentiteettimoduuleihin.

Kuviossa 1 esitettyyn tilaajaidentiteettimoduuliin (Subscriber Identity Module, SIM) kuuluu tietojenkäsittelylaite 1, kuten prosessori, mikrokontrolleri tai vastaava, muistilaite 2, joka on yhdistetty tietojenkäsittelylaitteeseen 1 ja tiedonsiirtolaite 3, joka on yhdistetty tietojenkäsittelylaitteeseen 1. Lisäksi tilaajaidentiteettimoduuliin SIM on järjestetty liityntärajapinta RP tiedon siirtämiseksi ulkoisen laitteen, kuten GSM-matkaviestimen ja tilaajaidentiteettimoduulin välillä.

Lisäksi kuviossa 1 esitettyyn tilaajaidentiteettimoduuliin kuuluu tai sinne on tallennettu sovellus APP, joka käyttää tilaajaidentiteettimoduulille tallennettuja varmenteita ollessaan yhteydessä palveluntarjoajan palveluihin. Edelleen tilaajaidentiteettimoduulille on järjestetty välineet 4 varmenteiden vastaanottamiseksi ja välineet 5 tietojen tallentamiseksi varmenteesta muistilaitteelle 2. Lisäksi tilaajaidentiteettimoduulilla on välineet 6 vastaanotetun varmenteen todentamiseksi oikeaksi mainitulla korttivarmenteella (CACert) ja välineet 7 oikeaksi todennetun varmenteen sisältämän varmenneketjun suodattamiseksi varmenteesta ennen varmenteen tallentamista.

Edelleen kuviossa 1 esitetty tilaajaidentiteettimoduuli käsittää välineet 8 tilaajaidentiteettimoduulille tallennetun varmenteen Mcert_1 varmentamiseksi korttivarmenteella CA_Cert ennen sen käyttämistä. Lisäksi tilaajaidentiteettimoduulilla on välineet

9 varmenteen hylkäämiseksi, jos se todennetaan epäluotettavaksi ennen tallentamista ja välineet 10 varmenteen hylkäämiseksi, jos varmenne todennetaan epäluotettavaksi ennen käyttöä. Edelleen tilaajaidentiteettimoduuli käsittää välineet 11 jokaiseen mainittuun varmenteeseen sisältyvän allekirjoituksen todentamiseksi ennen allekirjoituksen poissuodattamista.

Lisäksi kuviossa 1 on esitetty yllä olevaan esimerkkiin viitaten alueet A ja B, jotka siis ovat suojaamaton muistialue A ja suojattu muistialue B. Suojatulle muistialueella tallennetaan ainakin korttivarmenne Card_CA, joka käsittää korttivarmenteen antajan sähköisen tai verkkoidentiteetin, lyhyen nimikuvauksen varmenneviranomaisesta, varmenteen tyypin, esimerkiksi RSA, julkisen salausavaimen, julkisen allekirjoitusavaimen, varmenteen statuksen eli tiedon siitä, onko varmenne aktiivinen vai passiivinen ja lyhytsanomakeskuksen numero, joka viittaa varmenteen antajaan. Lisäksi suojatulle muistialueelle on tallennettu käyttäjän oma varmenne, joka voi esimerkinomaisesti käsittää muuten samat tiedot kuin edellä kuvattiin korttivarmenteen yhteydessä paitsi julkinen salausavain ja julkinen allekirjoitusavain korvataan salaisella salausavaimella ja salaisella allekirjoitusavaimella, vastaavasti. Käyttäjän varmenteeseen viitataan tässä esimerkissä termillä Mcert_1:llä. Lisäksi suojatulle muistialueelle B voidaan tallentaa palveluntarjoajien varmenteita, joista siis on suodatettu pois varmenneallekirjoitukset niiden varaaman muistialueen pienentämiseksi. Näihin varmenteisiin viitataan merkinnällä MCert_n. Myös näissä varmenteissa on edullisesti samat tiedot kuin korttivarmenteessa.

Seuraavaksi esitetään viitaten kuvioon 2 eräs edullinen toimintamalli vastaanotettaessa varmenne tilaajaidentiteettimoduulille. Ensin varmenne vastaanotetaan tilaajaidentiteettimoduulille, lohko 20. Var-

menne on korttivarmenteen antajan varmentama ja tämä tarkistetaan lohkossa 21. Jos havaitaan, että vastaanotettua varmennetta ei voida todentaa oikeaksi kortille tallennetulla korttivarmenteellakaan Card_CA, hylätään varmenne. Vaihtoehtoisesti proseduuri voitaisiin lopettaa tähän, mutta tässä esimerkissä voidaan pyytää varmenteen uudelleenlähetystä, lohko 25 ja sen jälkeen tarkistaa varmenne uudelleen. Tämä voidaan toistaa esimerkiksi kolme kertaa ja jos kolmannellakaan kerralla varmennetta ei todenneta oikeaksi, lopetetaan proseduuri.

Jos lohkossa 21 varmenne todennettiin oikeaksi, suodatetaan varmenteesta koko varmenneketju, jolloin jäljelle jää julkinen avain ja siihen liittyvä identiteetti ja mahdollisesti jotain muuta tietoa, lohko 23. Tämän jälkeen suodatettu varmenne tallennetaan, lohko 24, varmennetulle suodatetulle alueelle B-tilaajaidentiteettimoduulilla.

Seuraavaksi esitetään kuvioon 3 viitaten edullisia sanomarakenteita, joita voidaan käyttää keksinnön mukaisten varmenteiden lähettämiseksi ilmarajapinnan kautta tilaajaidentiteettimoduulille. Tässä esimerkissä oletetaan, että käytettävä sanomatyyppi on lyhtysanomaviesti (Short Message Service, SMS), mutta kuten ammattimiehelle on selvää, myös muita sanomamuotoja voitaisiin käyttää. Tässä esimerkissä varmenteen lähettämiseen käytetään kolmea lyhytsanomaviestiä, joissa on kuvion 3 mukainen sisältö.

Ensimmäinen lähetettävä sanoma on salaamaton (Non-encrypted SMS-message #1), jossa on kaksi kenttää. PublicKeyMod on julkinen verifiointi tai salausavain. Lisäksi viestissä on viestin järjestysnumero, MsgNumber. Tämän viestin pituus on yhteensä 1033 bittiä, jossa julkinen avain on 1025 bittiä ja sanomanumero 8 bittiä. Toisessa viestissä, Downloaded Data in message #2, on viisi kenttää. S3HDT Kuvaa viestin tyyppiä, ReceiverID vastaanottajan identiteettiä, Sen-

derID lähettäjän identiteettiä, jossa identiteetti voi olla esimerkiksi verkkoidentiteettitunnus, S3AP on osoitin, joka viittaa sovellukseen, joka kyseistä varmennetta käyttää, ja lisäksi viestiin kuuluu RSA-lohko, ENCDATA, joka on oletusarvoisesti allekirjoitettu ja salattu. Tämän viestin koko on 1120 bittiä.

Allekirjoitettu ja salattu data, ENCDATA, viestissä käsittää viisi kenttää, joista ensimmäisessä on RSA:n eniten merkitsevä bitti RSA_MSB, aloituskenttä, Start, satunnaisluvun juuri, Random, siirretty data SP_data ja Hash-tarkiste SP_data-kentän sisällöstä. Tarkisteella tarkistetaan tiedon eheys ja varmistetaan ettei tieto ole muuttunut lähetyksen aikana.

Edelleen SP_data viestissä #2 käsittää kahdeksan kenttää, joista ensimmäinen, NID, viittaa korttivarmenteen identiteettiin, Short Name viittaa avaimenhaltijan nimeen, Key Usage, avaimen käyttötarkoitukseen, KeyHash on tarkisteeseen viestistä numero 1, MCertHash tarkisteeseen varmenteesta, ja viestin numeron, MSG Number. Lopuksi lähetetään kolmas viesti, joka edelleen on viestin 2 ENCDATA SP_data-kenttää, jossa edelleen on osoitin korttivarmenteen antajan avainpariin NID, julkisen avaimen eksponentti, PublicKeyE ja viestin järjestysnumero MsgNumber. Huomautamme vielä, että edellä olevaa kuvausta edullisista sanomarakenteista ei ole tarkoitettu rajoittavaksi, vaan erääksi esimerkiksi keksinnön käytöstä. Kun todennetaan kortille tai tilaajaidentiteettimoduulille vastaanotettua varmennetta oikeaksi, käytetään yllä kuvattuja Hash-tarkisteita. Niiden avulla voidaan vakuuttua siitä, että vastaanotettu varmenne on tietyn ennalta määrätyn varmenneviranomaisen tai varmenteenantajan allekirjoittama ja varmentama. Kun varmenne on todettu oikeaksi, voidaan siitä poimia tai suodattaa julkinen avain ja siihen liittyvä identiteetti tallennettavaksi suodatetulle alueella B.

Esillä olevaa keksintöä ei rajata tässä esitettyihin esimerkkeihin, vaan monet muunnokset ovat mahdollisia pysyttäessä oheisten patenttivaatimusten määrittelemän suojapiirin rajoissa.

PATENTTIVAATIMUKSET

1. Menetelmä identiteettimoduulille tallennettujen varmenteiden hallitsemiseksi, joka identiteettimoduuli käsittää:

- tietojenkäsittelylaitteen (1),
- muistilaitteen (2), joka on yhdistetty mainittuun tietojenkäsittelylaitteeseen (1)
- muistilaitteelle tallennetun korttivarmenteen (CA),
- sovelluksen (APP), joka käyttää identiteettimoduulille tallennettuja varmenteita ja
- tiedonsiirtolaitteen (3), joka on yhdistetty mainittuun tietojenkäsittelylaitteeseen (1) ja johon on järjestetty liityntärajapinta (RP) tiedon siirtämiseksi ulkoisen laitteen ja identiteettimoduulin välillä, joka menetelmä käsittää seuraavat vaiheet:
- vastaanotetaan identiteettimoduulille varmenne, ja
- tallennetaan mainitusta varmenteesta tietoa mainitulle muistilaitteelle, t u n n e t t u siitä, että menetelmä edelleen käsittää vaiheen:
- todennetaan mainittu varmenne oikeaksi mainitulla korttivarmenteella ennen varmenteen tallentamista.

2. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että suodatetaan mainitusta oikeaksi todennetusta varmenteesta sen sisältämä varmenneketju.

3. Patenttivaatimuksen 1 tai 2 mukainen menetelmä, t u n n e t t u siitä, että varmennetaan mainittu varmenne korttivarmenteella ennen sen käyttämistä.

4. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että tallennetaan mainitusta varmenteesta sen sisältämä julkinen avain ja siihen liittyvä identiteetti.

5. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että hylätään mainittu varmenne,

jos se todennetaan epäluotettavaksi ennen sen tallentamista.

6. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että hylätään mainittu varmenne, jos se todennetaan epäluotettavaksi ennen sen käyttöä.

7. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että suodatusvaiheessa:

todennetaan jokainen mainittuun varmenteeseen sisältyvä allekirjoitus,

ja suodatetaan mainitusta varmenteesta vain oikeaksi todennetut allekirjoitukset.

8. Identiteettimoduuli varmenteiden hallitsemiseksi, joka identiteettimoduuli käsittää:

- tietojenkäsittelylaitteen (1),
- muistilaitteen (2), joka on yhdistetty mainittuun tietojenkäsittelylaitteeseen (1)
- muistilaitteelle tallennetun korttivarmenteen (CA),
- sovelluksen (APP), joka käyttää varmenteita,
- tiedonsiirtolaitteen (3), joka on yhdistetty mainittuun tietojenkäsittelylaitteeseen (1) ja johon on järjestetty liityntärajapinta (RP) tiedon siirtämiseksi ulkoisen laitteen ja identiteettimoduulin välillä, joka menetelmä käsittää seuraavat vaiheet,
- välineet (4) varmenteen vastaanottamiseksi identiteettimoduulille, ja
- välineet (5) mainitun varmenteen sisältämän tiedon tallentamiseksi mainitulle muistilaitteelle, t u n n e t t u siitä, että tilaajaidentiteettimoduuli edelleen käsittää:

välineet (6) mainitun varmenteen todentamiseksi oikeaksi mainitulla korttivarmenteella ennen varmenteen tallentamista.

9. Patenttivaatimuksen 8 mukainen identiteettimoduuli, t u n n e t t u siitä, että identiteettimoduuli edelleen käsittää

välineet (8) mainitun oikeaksi todennetun varmenteen sisältämän varmennusketjun suodattamiseksi varmenteesta.

10. Patenttivaatimuksen 8 mukainen identiteettimoduuli, t u n n e t t u siitä, että identiteettimoduuli edelleen käsittää välineet (8) mainitun varmenteen varmentamiseksi korttivarmenteella ennen sen käyttämistä.

11. Patenttivaatimuksen 8 mukainen identiteettimoduuli, t u n n e t t u siitä, että identiteettimoduuli edelleen käsittää välineet (9) mainitun varmenteen hylkäämiseksi, jos se todennetaan epäluotettavaksi ennen sen tallentamista.

12. Patenttivaatimuksen 8 mukainen identiteettimoduuli, t u n n e t t u siitä, että identiteettimoduuli edelleen käsittää välineet (10) mainitun varmenteen hylkäämiseksi, jos se todennetaan epäluotettavaksi ennen sen käyttämistä.

13. Patenttivaatimuksen 8 mukainen identiteettimoduuli, t u n n e t t u siitä, että identiteettimoduuli edelleen käsittää välineet (11) jokaisen mainittuun varmenteeseen sisältyvän allekirjoituksen todentamiseksi ennen suodatusta.

(57) TIIVISTELMÄ

Keksinnön kohteena on menetelmä identiteettimoduulille tallennettujen varmenteiden hallitsemiseksi. Menetelmässä vastaanotetaan identiteettimoduulille varmenne, ja tallennetaan mainitusta varmenteesta tietoa identiteettimoduulille. Keksinnön ansiosta identiteettimoduulille voidaan tallentaa aiempaa useampia varmenteita.

(Fig. 1)

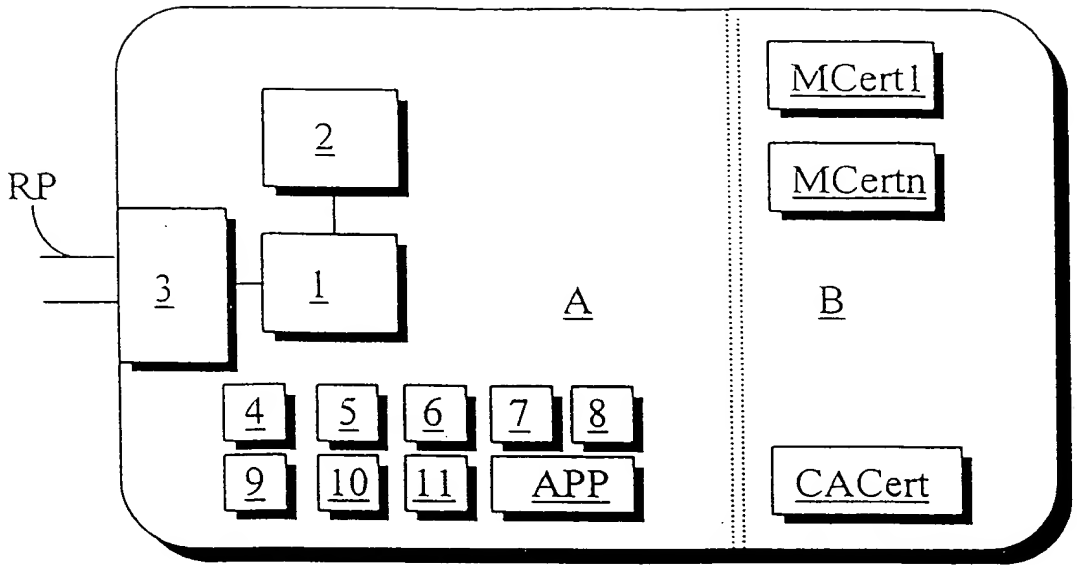

RP
2
3
1
A
B
MCert1
MCertn
4
5
6
7
8
9
10
11
APP
CACert

Fig. 1

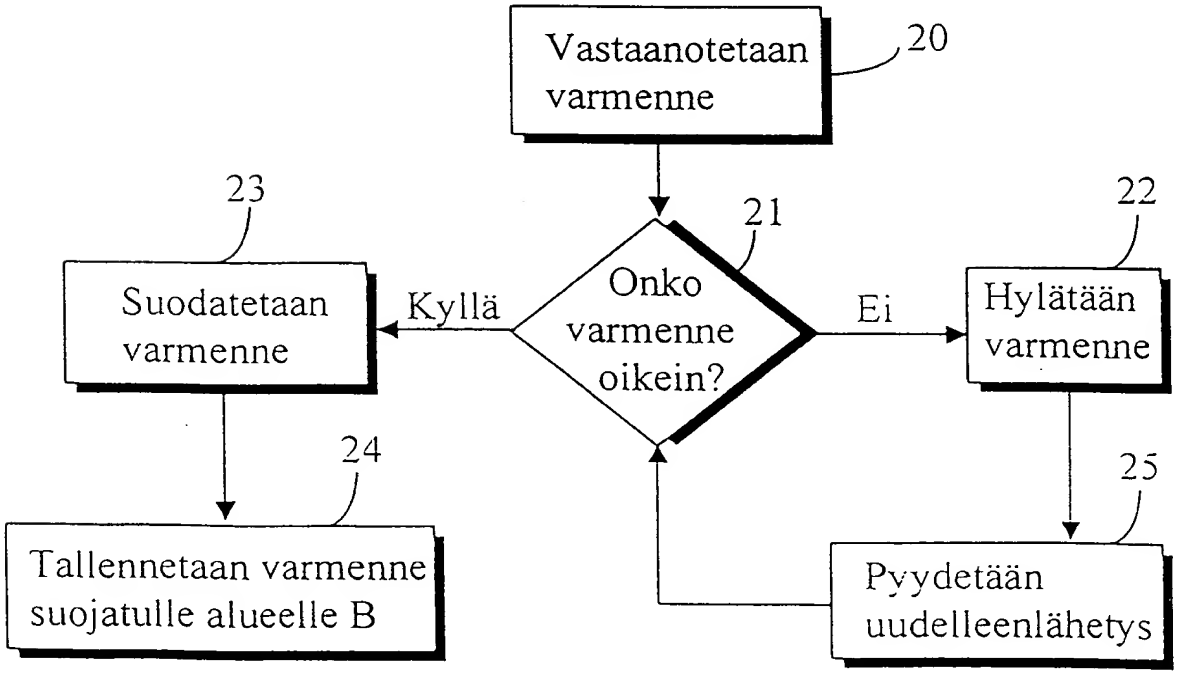
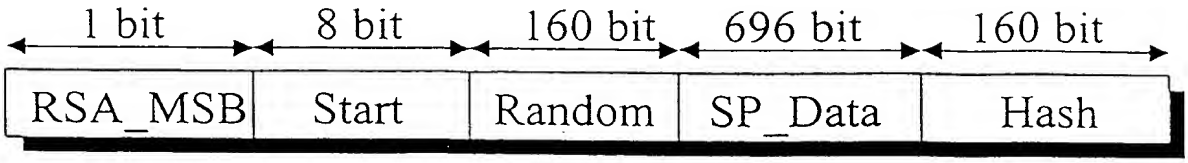
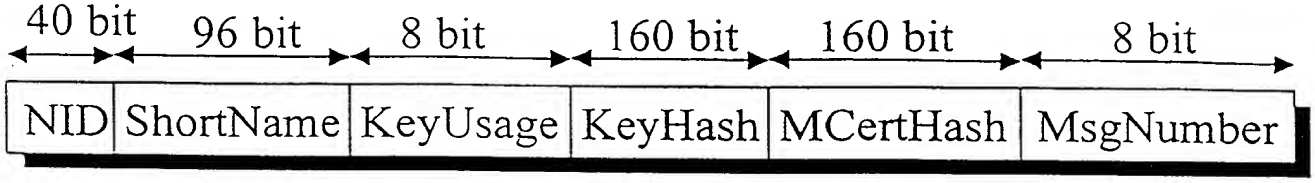

Vastaanotetaan varmenne
20
23
21
22
Suodatetaan varmenne
Kyllä
Onko varmenne oikein?
Ei
Hylätään varmenne
24
25
Tallennetaan varmenne suojatulle alueelle B
Pyydetään uudelleenlähetys

Fig. 2

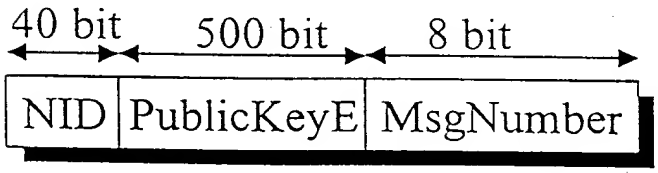
EncData in message#2 (1025 bit)



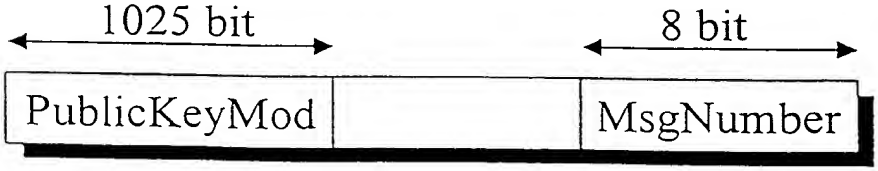
SP_Data in message#2 (696 bit)



SP_Data in message#3 (548 bit)



Non encrypted SMS-message#1



Downloaded Data in message#2

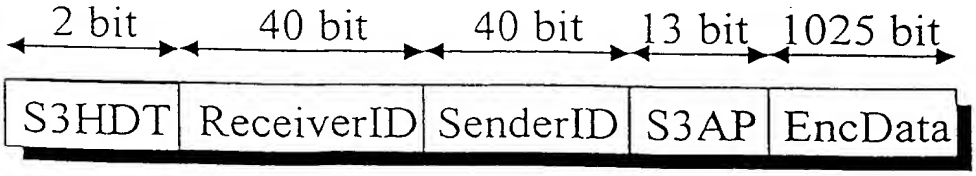


Fig. 3